Developing a Security Exposure Self-Assessment Tool

Candace Sands (EMA) & Matt Earley (DAC)

PCSF Fall Meeting

October 27, 2005

OUTLINE

- Project Background
- Project Team and Stakeholders
- Research Objectives & Scope
- Technical Approach & Methodology
- Next Steps
- **Q&A**

PROJECT BACKGROUND

- There are approximately 160,000 public water systems (PWSs) in the U.S.
- About 84% of the total U.S. population is served by PWSs, or ~273 million out of a total population of 290 million (as of 2003).
- The U.S. wastewater infrastructure includes over 16,255 publicly owned treatment works (POTWs) and nearly 100,000 pumping stations
- 2.3 million miles of system pipes
- 75% of the total U.S. population is served by POTWs
- POTWs treat 32 billion gallons of wastewater every day
- Securing the electronic / automated systems needed to run these organizations would be a substantial undertaking

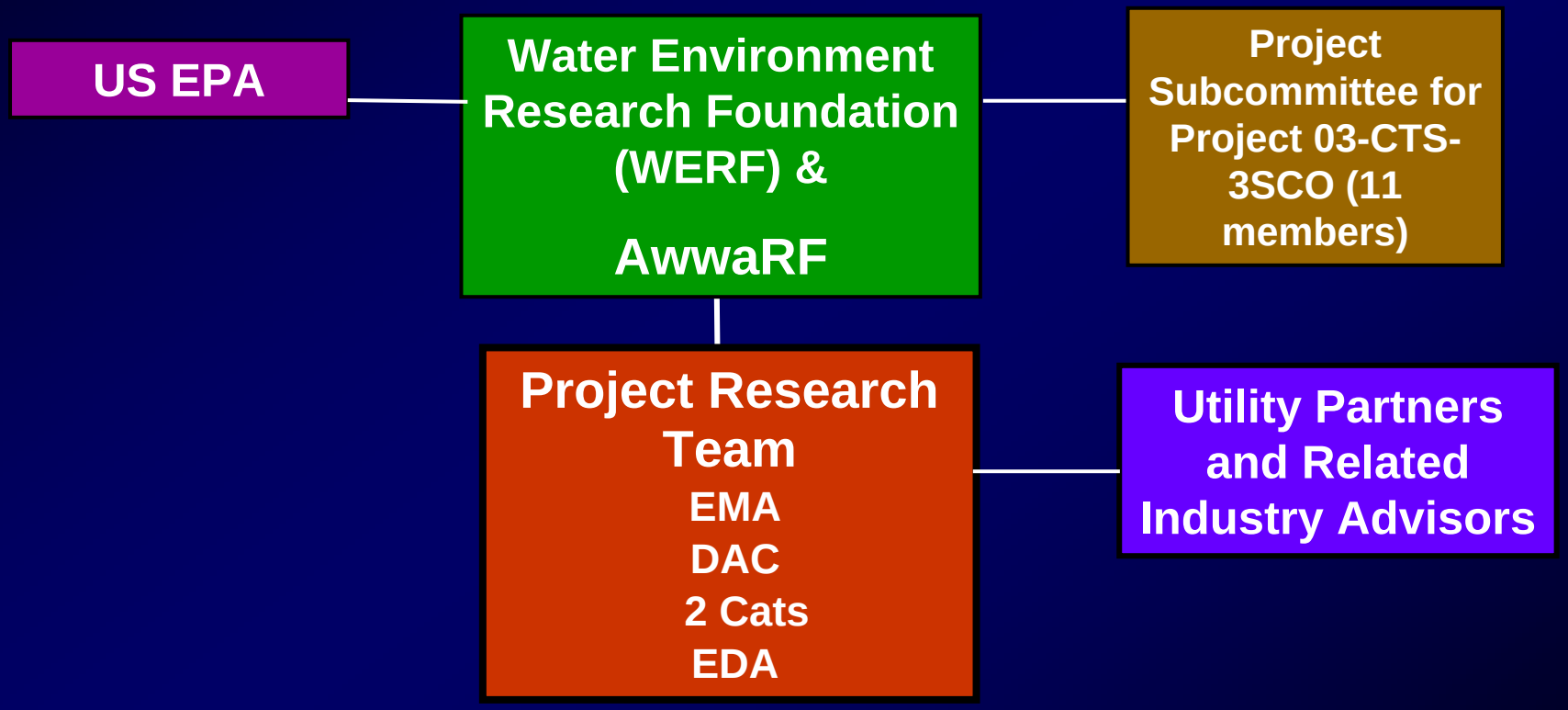
PROJECT BACKGROUND, cont.

- In September 2002, WERF was awarded, by the U.S. EPA Water Security Division, a grant covering a spectrum of projects including *Project 03-CTS-3SCO: Security Measures for Computerized and Automated Systems at WW Facilities*
- AwwaRF joined the research sponsor team in January 2004
- Research scope expanded to also include water facilities

PROJECT BACKGROUND, cont.

- Key Objectives of the EPA Security Grant:
  - Address multiple spectrum of issues related to security (public health, vulnerability, protection of water and wastewater infrastructure, and communications)
  - Develop Emergency Response Plans for use by water/wastewater utilities

PROJECT TEAM



PROJECT RESEARCH TEAM

- Candace Sands, PI/PM
- Bob George
- Bob Hill, PhD

- Ron Melton, PhD
- Matt Earley

- Alicia Crumpton

- Elizabeth Davidson

UTILITY PARTNERS & EXPERT ADVISORS

- Columbus Water Works, GA
- DC WASA, DC
- JEA, FL
- Madison, WI
- Metro Denver, CO
- Passaic Valley Sewerage Commissioners, PA
- *MWRA, MA*
- Phoenix WSD, AZ
- Sacramento CRSD, CA
- Union Sanitary District, CA

- *GTI – Bill Rush*
- *EPRI – Tom Kropp*
- *IWA ICA Committee – John Andrews*
- *NSF – Mariam Heller*

RESEARCH OBJECTIVES

1. Adapt a RA methodology to determine current vulnerabilities, consequences, and quantify relative risks for the W/WW communities.
2. ID and prioritize security weaknesses in computerized and automated systems (e.g., control system) – including technology, people, policies & procedures, & data security both within the plant and remote networks.
3. Clarify the data communication options within a utility network – i.e., incl. standards-based data communication methods, protocols, equip & S/W.

RESEARCH OBJECTIVES, cont.

4. Identify electronic operation and data security standards and practices that can be applied to W/WW systems.
    - Standards addressing the issues of weakness & build upon the options identified
    - Use of ISO 15408:1999 Common Criteria and expanded guidelines and specifications under development through NIST Process Control Security Requirements Forum (PCSRF)
5. Develop best practices for secure data communication - that allow utilities to choose data communication methods that best fit their systems.

RESEARCH OBJECTIVES, cont.

6. Validate best practice, security guidance, & specification with utility partners and revise as needed.
7. Adapt public domain and/or commercially available assessment and decision-making tools for easy use at the utility level.
8. Provide proof-of-concept where possible by documenting successful implementation of each options - list strengths and weaknesses of each approach.
9. Bring in experience from other related sectors – Electric, Gas, Industrial, etc.

MULTI-YEAR SCOPE

- 2 Year Duration - started Sept 2004

Phase I

- Secondary Research and Assessment Tool
- Guidelines Development, Validation, & Adapt Tool

Phase II

- Apply (Pilot) and Adjust
- Update Guidelines

PROGRESS TO DATE

- Completed Secondary Research task and prepared an interim draft of findings, statuses, and trends
- Conducted material research efforts, designed and developed a Beta version of the Control System Security Measures Self Assessment Tool (CS SESAT)
- Performed QA and internal validation (research team) of the approach and methodology used in the design and development of the tool
- Utility Partners performed Beta testing/review
- Designed methodology for and conducted on-site field assessments
- Implemented Security Measures Workshop in Washington, D.C. in April 2005
- Started drafting leading practices, recommendations, and guidance document

TECHNICAL APPROACH

CS SESAT DEVELOPMENT GOALS

- Comprehensive & systematic methodology.
- Leverage well established tools & methodologies (e.g., material from secondary research).
- Scalability - capable of being applied at large utilities & smaller utilities.
- Incorporation into integral long term security (physical & cyber) strategy.
- Easy to use - with little or no experience with security assessments.
- Delivery – readily useable and acceptable within utilities (i.e., Microsoft Excel).
- Repeatability - over time by different users.

SELF ASSESSMENT FUNDAMENTALS

- Avoid vendor- or product-centric approach to security
- Material identified from secondary research (e.g. NIST 800-26, ISO/IEC 17799, ISO/IEC 15408, ISA SP-99, Sandia RAM-W^{SM}, VSAT)
- NIST Process Control Security Requirements Forum (PCSRF) provides structured approach to evaluation of system/device security
  - Provides approach to capture unique process control security requirements (e.g. System Protection Profile – Industrial Control Systems)

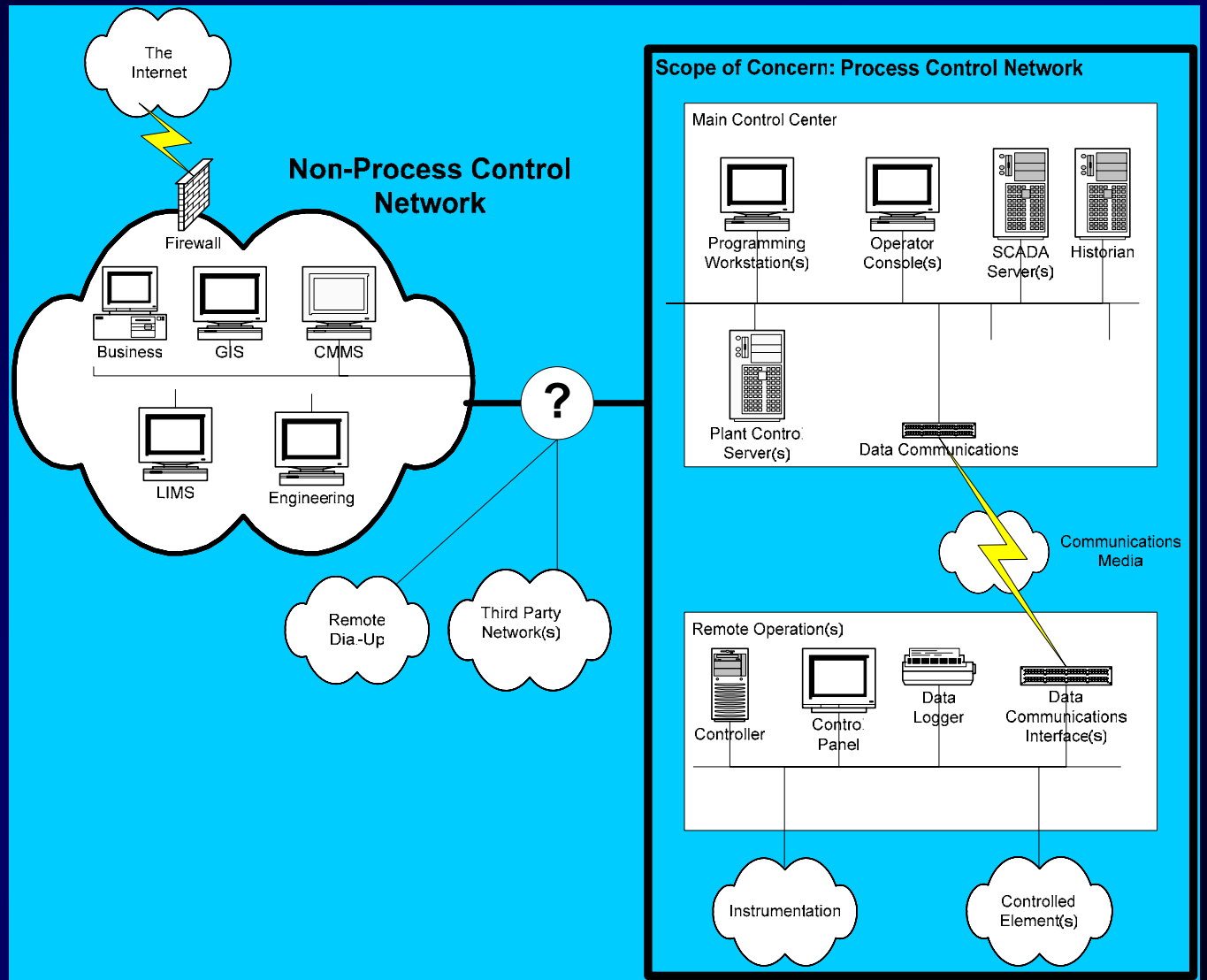
A *SIMPLE* SELF ASSESSMENT PROCESS

- Minimal organizational investment
  - 2 to 5 day completion (approx)
  - User friendly (questionnaire based)
  - Less reliance on external consultants
- Balanced approach to Security
  - Risk Assessment
    - Technical Controls
    - Operational Controls
    - Management Controls

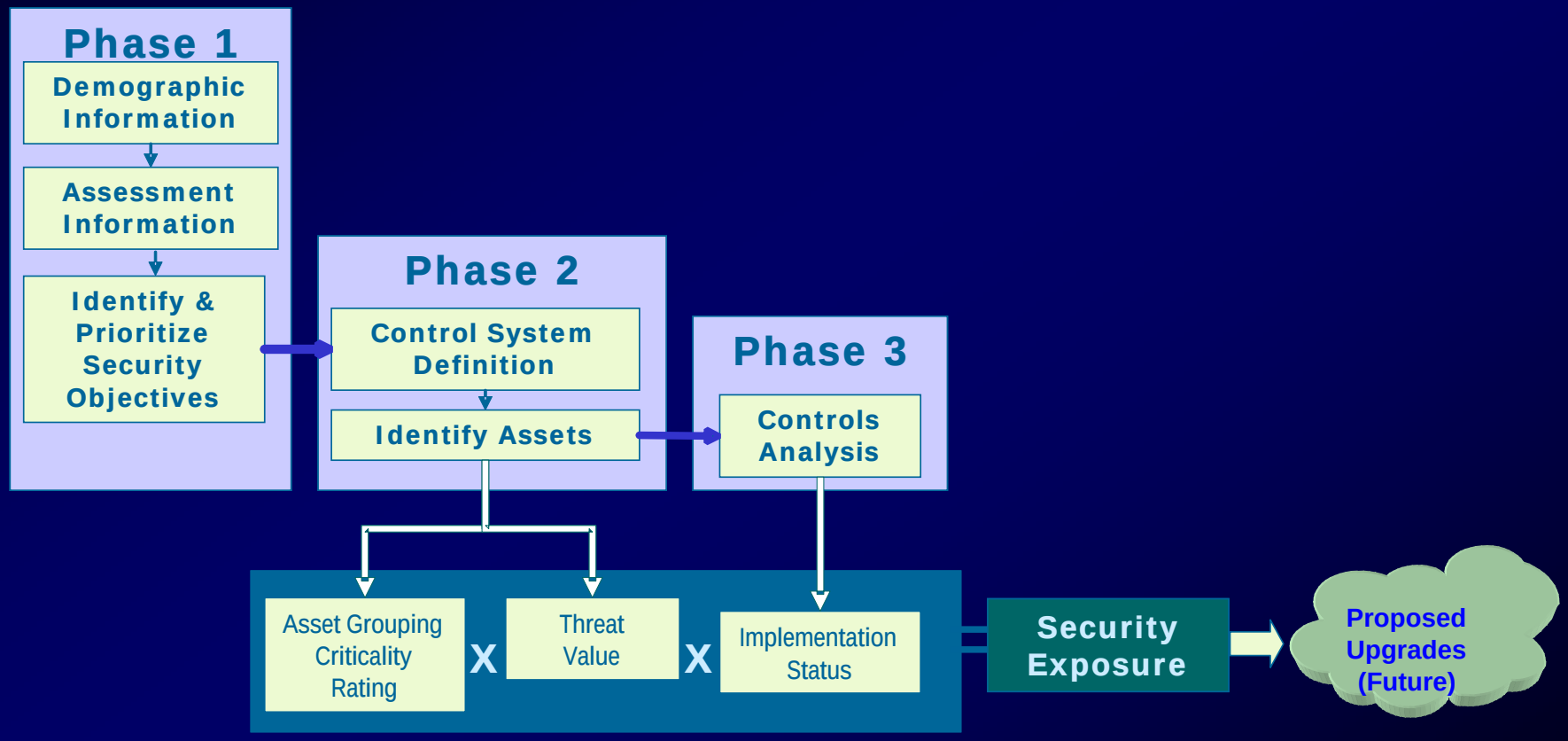
FOUNDATION FOR SELF ASSESSMENT

- Generally accepted process control definition
- Focus on the critical components within the process control system
- Scope: Process Control Systems (e.g. SCADA) and any *relevant systems*
  - Interaction of other business applications deployed within the enterprise network (e.g. CMMS, CIS, GIS, etc) – DATA ONLY

Process Control System Model



SECURITY EXPOSURE SELF ASSESSMENT METHODOLOGY



UTILITY INVOLVEMENT

10 Utilities Complete Assessment

↓

4 Utilities Participate In Depth Field Assessment

↓

Data Analysis

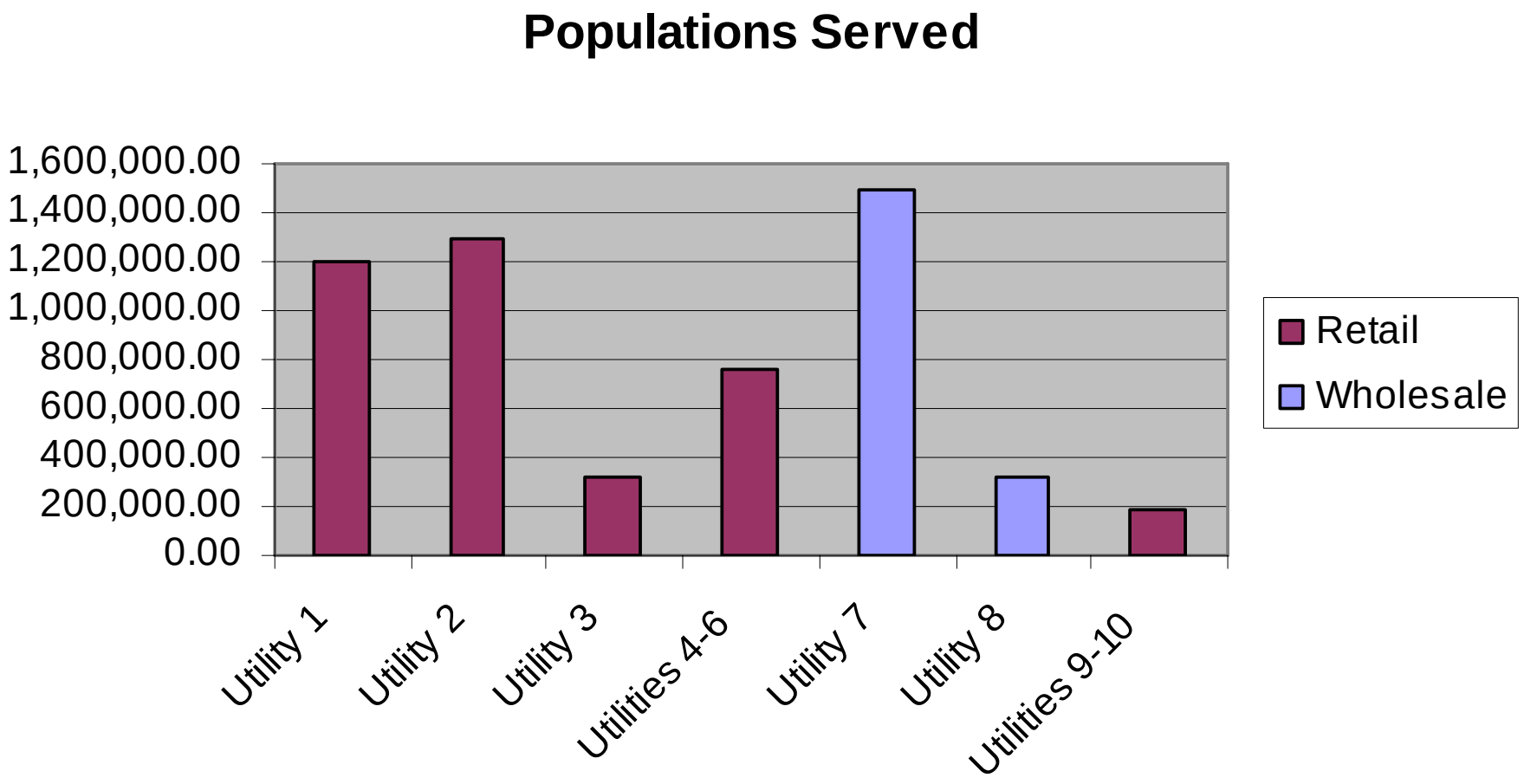
↓

Security Management Workshop Presents Tool Implementation Results

Data Analysis

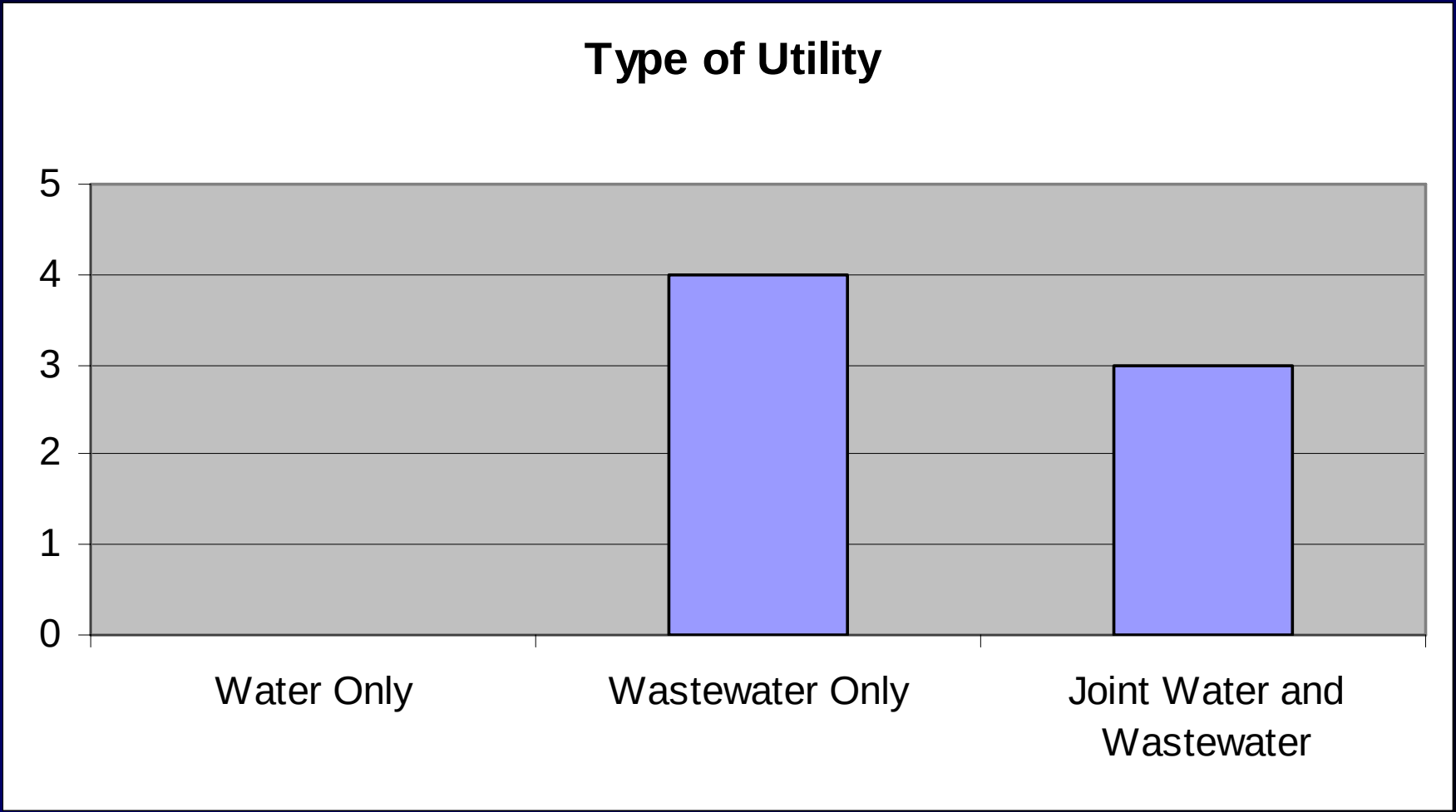
- Comparative analysis across respondents
- Looking for industry
  - Consistency
  - Good practices (strengths)
  - Bad practices (weaknesses)
- Self-consistency of individual utility's responses

Demographics



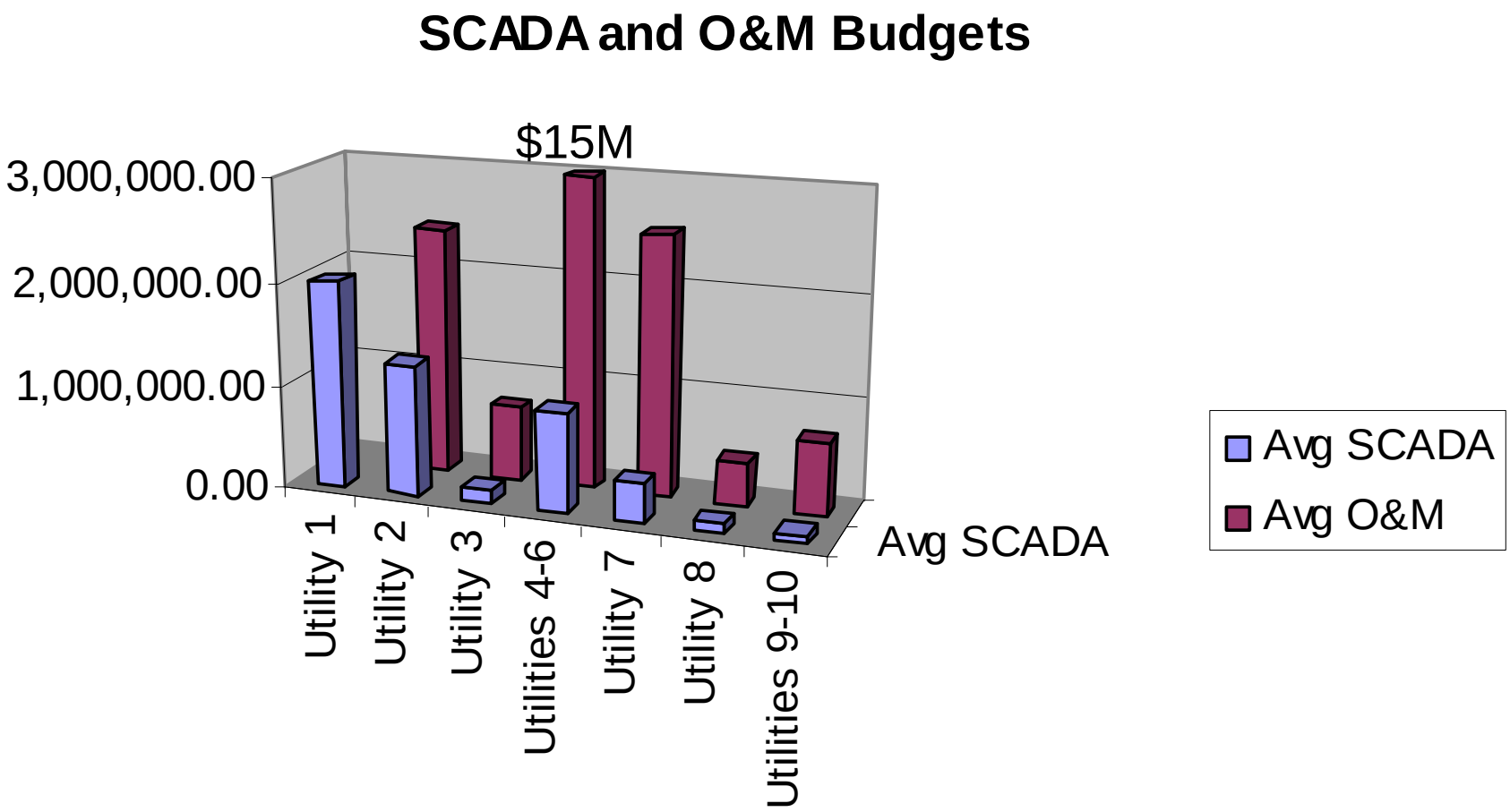
Demographics

Joint or Wastewater Only – No Water Only



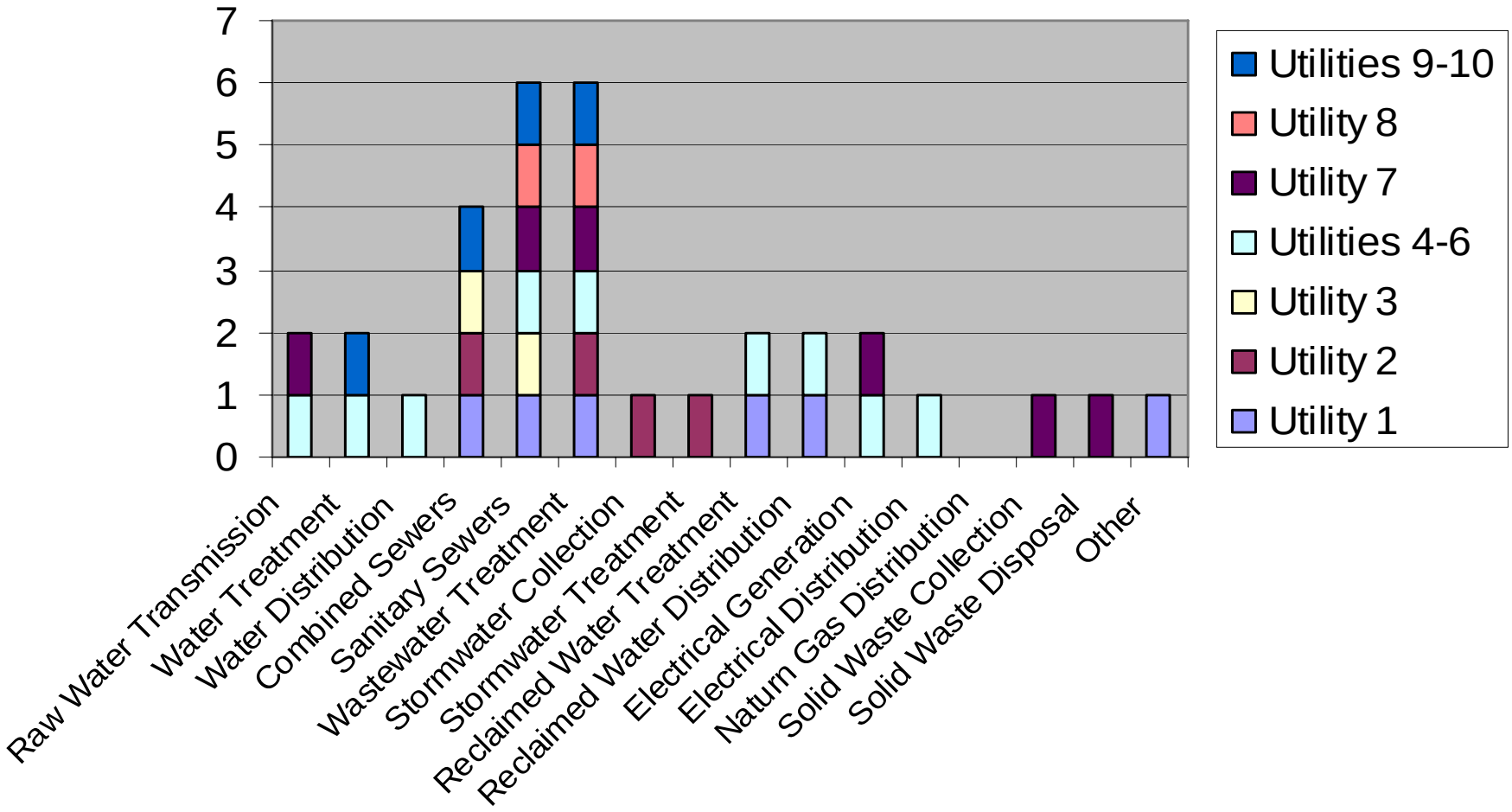
Demographics

Control System and O&M Budgets



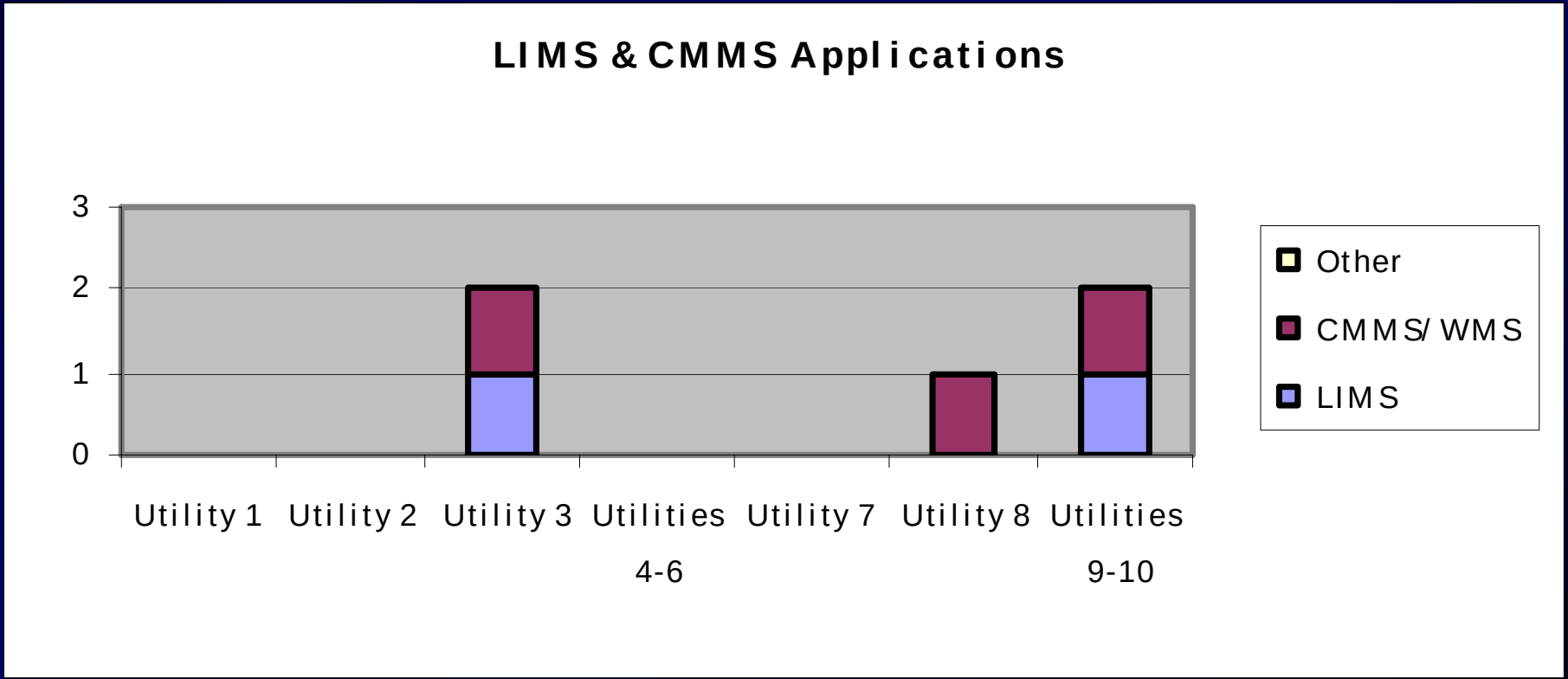
Demographics

Provide a Wide Variety of Services



Demographics

Several Laboratory and Maintenance Management Applications



Demographics

Few Other Applications

- No Customer Service Applications
- No Engineering Applications
- No Financial Applications
- No Fleet Applications
- No Human Resource Applications
- No Procurement Applications

Data Analysis – Common Areas of Security Exposure

- Security Policy
- Change Management
- Dial-up / Remote Users
- Account Management
- Event Monitoring & Intrusion Detection
- Disaster Recovery
- Internet
- Wireless
- Remote Sites

Summary Results – Main Questions

	021005A	021105A	021105B	021405A1	021405A2	021405A3	021405B	021505A	021605A1	021605A2	***Average***
Security Policy	0.08		0.16	0.24	0.33	0.18	0.16	0.16	0.06	0.27	*0.18*
Security Officer & Organization	0.08		0.08	0.16	0.13	0.14	0.04	0.08	0.02	0.07	*0.09*
Awareness & Training	0.04		0.10	0.06	0.18	0.06	0.09	0.12	0.03	0.14	*0.09*
Recruitment Process	0.03		0.05	0.00	0.00	0.00	0.04	0.08	0.02	0.09	*0.04*
Employee Exit/Transfer	0.04		0.04	0.02	0.07	0.02	0.00	0.00	0.01	0.04	*0.03*
Change Management	0.07	0.00	0.03	0.19	0.21	0.19	0.13	0.15	0.06	0.25	*0.13*
Router/Firewall	0.07	0.05	0.09	0.15	0.08	0.07	0.02	0.10	0.00	0.00	*0.06*
Dial-up/ remote users	0.09	0.09	0.24	0.12	0.22	0.00	0.17	0.16	0.04	0.17	*0.13*
Third party connections	0.11	0.12	0.00	0.05	0.06	0.05	0.08	0.00	0.01	0.05	*0.05*
Application Security Analysis	0.03	0.03	0.04	0.05	0.08	0.05	0.01	0.08	0.01	0.03	*0.04*
Access Control/Directory Services	0.01	0.00	0.03	0.05	0.00	0.00	0.02	0.06	0.00	0.00	*0.02*
Security in Application Development	0.04	0.00	0.06	0.07	0.03	0.02	0.07	0.10	0.02	0.09	*0.05*
Data Security	0.05	0.03	0.01	0.09	0.10	0.02	0.00	0.04	0.01	0.03	*0.04*
Data Classification	0.03	0.00	0.01	0.02	0.02	0.02	0.04	0.01	0.01	0.03	*0.02*
Data Encryption	0.05	0.05	0.04	0.04	0.07	0.06	0.02	0.07	0.01	0.06	*0.05*
Server Vulnerability & Hardening	0.04	0.00	0.05	0.02	0.05	0.00	0.04	0.04	0.00	0.00	*0.02*
Server Backup	0.05	0.00	0.00	0.00	0.14	0.12	0.01	0.00	0.00	0.00	*0.03*
Use of Laptops or Other Portable Devices	0.04	0.03	0.05	0.05	0.05	0.05	0.03	0.08	0.01	0.03	*0.04*
System Security Risk Management	0.05	0.02	0.06	0.07	0.08	0.07	0.00	0.08	0.02	0.09	*0.06*
Account Management	0.12	0.14	0.12	0.07	0.08	0.07	0.16	0.15	0.03	0.11	*0.10*
Password Management & Authentication	0.07	0.05	0.08	0.04	0.05	0.04	0.05	0.10	0.04	0.16	*0.07*
Event Monitoring & Intrusion Detection	0.15	0.22	0.14	0.24	0.27	0.24	0.19	0.29	0.06	0.26	*0.21*
Incident Response	0.05	0.06	0.06	0.07	0.07	0.07	0.02	0.03	0.01	0.07	*0.05*
Disaster Recovery	0.09	0.20	0.11	0.06	0.12	0.10	0.02	0.16	0.05	0.24	*0.11*
Physical Security - Buildings & Client Machines	0.09	0.03	0.04	0.07	0.07	0.04	0.12	0.09	0.03	0.13	*0.07*
Physical Security - Server Rooms	0.07	0.01	0.00	0.05	0.03	0.03	0.00	0.06	0.00	0.00	*0.03*
Asset Inventory	0.11	0.02	0.07	0.00	0.09	0.00	0.06	0.00	0.01	0.06	*0.04*
Software Management	0.11	0.01	0.04	0.03	0.00	0.00	0.00	0.00	0.01	0.03	*0.02*
VPN - Remote User Connectivity		0.04	0.00	0.07	0.00	0.00	0.00	0.00	0.01	0.02	*0.01*
VPN - Site to Site Connectivity	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	*0.00*
Internet	0.00	0.20	0.09	0.09	0.16	0.14	0.07	0.14	0.02	0.09	*0.10*
Outsourcing	0.16	0.00	0.15	0.00	0.00	0.00	0.28	0.12	0.04	0.16	*0.09*
Voice		0.00	0.10	0.19	0.00	0.00	0.18	0.00	0.00	0.00	*0.05*
Wireless			0.29					0.15	0.04	0.19	*0.17*

Summary Results – Remote Ops

	021005A	021105A	021105B	021405A1	021405A2	021405A3	021405B	021505A	021605A1	021605A2
Remote Site #1	0.16		0.09	0.13	0.35	0.12	0.12	0.12	0	0.06
Remote Site #2			0.09			0.17	0.12	0.12	0	0.06
Remote Site #3						0.12	0.12	0.17		0.06
Remote Site #4						0.12				
Remote Site #5										
Mean	0.115									
Standard Error	0.0163									
Median	0.12									
Mode	0.12									
Standard Deviation	0.0727									

KEY FINDINGS RELATED TO THE TOOL

- No one “picture” captures all variations of Utility process control networks
- Wide variation on use and meaning of terms
- Boundaries of process control systems often blurred
- Need to include relative risk assessment
- Business case/justification for improvements is important

OBSERVATIONS

- Compliance to government mandates not seen as critical
- Security awareness improved through use of risk assessment tools (e.g. VSAT)
- Lack of total trust in automated systems (operators still validate critical indicators)
- System Diagnostics not seen as critical due to impact on system availability

OBSERVATIONS

- Interactions with business applications limited but still lacking depth of protection
- Remote access limited but still not conformant with Leading Practices
- False sense of security from reliance on proprietary protocols and systems

NEXT STEPS

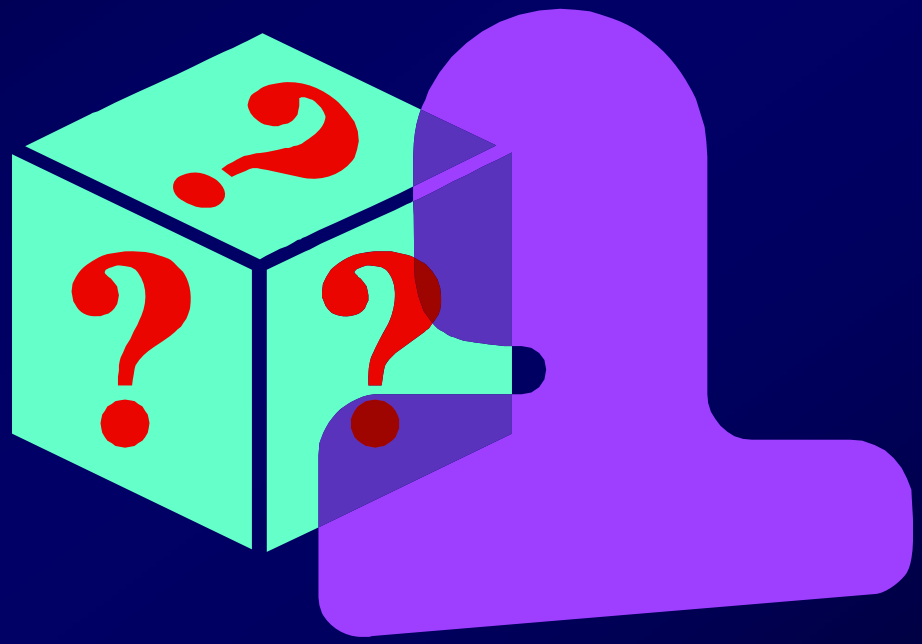
MULTI-YEAR SCOPE - ENHANCED

- In September 2005 - US EPA, DHS, INL, WERF agreed to collaborate with DHS NCSD Industrial Control Cyber Security program
- Develop tool customizations focused on the water / wastewater sector
- INL tool and CS SESAT have been designed to support this collaboration
- Customizations based on our experience with CS SESAT

MULTI-YEAR SCOPE - ENHANCED

- Validate with selected groups of utilities
- Modify and refine the tool
- Develop and deliver sector focused training covering the security model, the tool, and the application of both to the water / wastewater sector
- Collaboration keeps original project timeline intact
- Start November 2005

QUESTIONS & ANSWERS



Contact Information

- Candace Sands – EMA
  - csands@ema-inc.com
  - 520.299.0992
- Matt Earley – Decisive Analytics Corporation
  - matt.earley@dac.us
  - 410.884.7000 x232